1, 2 (canceled).

3. (previously presented) The method of Claim 17, wherein the combination is a hash function of a concatenation of the channel key K_c and session key K_s.

4-6 (canceled).

7. (previously presented) The method of Claim 17, wherein at least one of the providing acts is undertaken in a point-to-point communication.

8. (previously presented) The method of Claim 17, wherein at least one of the providing acts is undertaken as part of a broadcast.

9-11 (canceled).

12. (previously presented) The method of Claim 17, comprising selectively updating the session key block.

13. (original) The method of Claim 12, comprising updating the session key block by encrypting an updated session key with at least the encryption scheme B^R_{s1}.

14. (canceled).

15. (previously presented) The method of Claim 17, wherein the new channel key K_c' is sent in a message that is split.

16. (previously presented) The method of Claim 17, wherein the new channel key K_c' is refreshed using plural messages.

17. (previously presented) A computer-implemented method for securely transmitting multicast data, comprising:

encrypting at least one title T with at least title key K_T; and

encrypting the title key K_T with at least one channel-unique key K_{cu} using at least one encryption function S to render a multicast data channel encrypted as $S_{Kcu}(K_T)$, $S_{KT}(T)$, wherein the channel-unique key K_{cu} is the result of a combination of a channel key K_c and a session key K_s, wherein the session key K_s is encrypted with at least a first encryption scheme B^R_{s1} to render a session key block, further comprising providing at least one player with device keys K_d to activate the player and providing the player with the channel key K_c and the session key block, wherein the player can determine the session key K_s from the session key block using the device keys K_d, further comprising periodically refreshing the channel key K_c to enforce subscriptions, wherein a new channel key K_c' is encrypted with at least a second encryption scheme B^R_{s2} and wherein the encryption scheme B^R_{s2} includes:

assigning each player in a group of players respective private information I_u;

partitioning players not in a revoked set R into disjoint subsets $S_{i1},...S_{im}$ having associated subset keys $L_{i1},...L_{im}$; and

encrypting the session key K_S with the subset keys $L_{i1},...,L_{im}$ to render m encrypted versions of the session key K_S.

18. (original) The method of Claim 17, wherein the encryption scheme B^R_{s2} further includes partitioning the players into groups $S_1,...,S_w$, wherein "w" is an integer, and the groups establish subtrees in a tree.

19. (original) The method of Claim 18, wherein the tree includes a root and plural nodes, each node having at least one associated label, and wherein each subset includes all leaves in a subtree rooted at some node v_i that are not in the subtree rooted at some other node v_j that descends from v_i.

20. (original) The method of Claim 19, wherein the revoked set R defines a spanning tree, and wherein the method includes:

initializing a cover tree T as the spanning tree;

iteratively removing nodes from the cover tree T and adding nodes to a cover until the cover tree T has at most one node.

21. (original) The method of Claim 19, wherein each node has at least one label possibly induced by at least one of its ancestors, and wherein each player is assigned labels from all nodes hanging from a direct path between the player and the root but not from nodes in the direct path.

22. (original) The method of Claim 21, wherein labels are assigned to subsets using a pseudorandom sequence generator, and the act of decrypting includes evaluating the pseudorandom sequence generator.

23-48 (canceled).